多数決関数を計算する2層の多数決回路について (アルゴリズムと計算理論の基礎と応用)

AUTHOR(S):

吉田, 昌史; 天野, 一幸

CITATION:

吉田, 昌史 ...[et al]. 多数決関数を計算する2層の多数決回路について (アルゴリズムと計算理論の基礎と応用). 数理解析研究所講究録 2018, 2088: 1-8

ISSUE DATE:

2018-08

URL:

http://hdl.handle.net/2433/251591

多数決関数を計算する2層の多数決回路について

吉田 昌史 *　天野 一幸 †
群馬大学 大学院理工学府
Masafumi Yoshida　Kazuyuki Amano
Dept. of CS, Gunma University

概 要

n 変数多数決関数 $\mathrm{MAJ}_n : \{0,1\}^n \to \{0,1\}$ とは，0 または 1 を示す変数を n 個入力とし，その半数以上が 1 であるとき，かつそのときに限り 1 を出力する論理関数である．本研究では，MAJ_n を，$m < n$ に対する MAJ_m 素子を 2 層重ねた回路で構成する問題を考える．コンピュータ探索を用いて $(n,m) = (7,5)$ における全探索を行い，得られた結果の一般化を通じて $(n,m) = (n,n-2)$ に対して本質的に異なる 3 通りの多数決回路の構成を与える．

1　はじめに

n 変数多数決関数 $\mathrm{MAJ}_n : \{0,1\}^n \to \{0,1\}$ とは，n 個の 0 または 1 の入力をとり，その半数以上が 1 であるとき，かつそのときに限り 1 を出力する論理関数である．

多数決関数を計算する (あるいは近似する) 効率の良い論理回路を構成しようという研究は，古くから多く行われている．例えば，Valiant [8] による，入次数 2 の AND，OR ゲートからなる深さ $\sim 5.3 \log n$ の回路の確率的な構成法はこれに関する最も美しい結果の一つである．(他にも，例えば [1, 5, 7] や，より詳細な背景については [3] あるいは [4] の序章を参照されたい.)

最近，Kulikov や Podolskii は，この問題の「ダウンスケール版」として，n 変数多数決関数を小さな定数段数 (特に 2 段) の m $(< n)$ 入力多数決ゲートで計算する回路についての研究を始めた [4]．ここで，多数決関数を計算するゲートを多数決ゲートと呼び，また，m 入力多数決ゲートを 2 層重ねた回路を $\mathrm{MAJ}_m \circ \mathrm{MAJ}_m$ と表す．特に，MAJ_n が $\mathrm{MAJ}_m \circ \mathrm{MAJ}_m$ 回路により計算可能となるような m の最小値を求める問題は，単純ではあるが非常に興味深い．例えば，$(n,m) = (7,5)$ という非常に簡単なケースでさえ，このような回路が存在するか否かは自明ではない．

彼らは，文献 [4] において，m に対する下界 $m \geq n^{13/19+o(1)}$ を示すとともに，計算機による探索により，$(n,m) = (7,5), (9,7), (11,9)$ に対する具体的な回路の構成法を発見した．一方，この構成法を一般化し，$n > 11$ に対する m の非自明な上界を与えることは，未解決問題として残されていた．

本稿では，この問題に答え，任意の奇数 $n \geq 7$ に対して，$(n,m) = (n,n-2)$ を満たす $\mathrm{MAJ}_m \circ \mathrm{MAJ}_m$ 回路が存在することを，具体的な回路を提示することで証明する．また，本稿では，1 種類の構成法のみではなく，3 種類の本質的に異なる構成法を与える [1]．本研究では，$(n,m) = (7,5)$ に対して計算機を用いた全数探索を行い，得られた結果から一般的な回路を類推するアプローチにより，これを実現した．

なお，m に対する下界は，その後，1 層目のゲートが各入力変数を複数回読まないという条件のもと

*yoshida_masafumi@amano-lab.cs.gunma-u.ac.jp
†amano@gunma-u.ac.jp

[1] 3 種の回路のうち 1 つについては，[2] にも記載されている．

で，Engels らにより $m = \Omega(n^{0.8})$ に改良されている [3]．また，より一般的なしきい値素子を用いた結果は [6] にも述べられている．

2　準備

2.1　多数決関数と多数決回路

n 変数多数決関数 $\mathrm{MAJ}_n : \{0,1\}^n \to \{0,1\}$ とは，0 または 1 を示す変数を n 個入力とし，その半数以上が 1 であるとき，かつそのときに限り 1 を出力する論理関数であり，以下のように表される．

$$\mathrm{MAJ}_n(x_1, \ldots, x_n) \quad = \quad \mathbf{1}[\sum_{1 \le i \le n} x_i \ge n/2]$$

ここで，$\mathbf{1}[\ldots]$ は，括弧内の条件が真のとき 1 を，それ以外のとき 0 を与えるものとする．つまり MAJ_n は，$(x_1, ..., x_n$ における 1 の数$) \ge (x_1, ..., x_n$ における 0 の数$)$ のとき 1 を出力し，それ以外のとき 0 を出力する．

多数決回路とは，多数決ゲートが 2 層以上連なり回路となったものを指す．多数決ゲートとは，多数決関数を計算するゲートのことである．多数決回路も多数決関数と同様に，入力に対して多数決の計算を行い，正しい多数決の結果を出力する．

本稿では，専ら 2 層の多数決回路を扱う．入力側に近いゲートを単に **1 層目のゲート**と呼ぶ．それぞれの 1 層目のゲートは，変数 $\boldsymbol{x} = \{x_1, x_2, \ldots, x_n\}$ のいくつかを入力とし，それらの値の多数決を計算する．その後，出力ゲートが各 1 層目ゲートの出力の多数決を計算し，回路全体の出力とする．

2 層の $(n-2)$ 多数決回路とは，1 層目のゲートと出力ゲートで構成され，かつ回路における入力数と各ゲートの入力数との差が 2 の多数決回路のことである．本稿では，この形の回路のみを扱う．この回路は 1 層目ゲートのそれぞれの出力を出力ゲートへの入力とするため，1 層目ゲートの数は $n-2$ 個となる．

3　2 層の多数決回路探索

本研究では，入力数 $n-2$ における 2 層の多数決回路の探索を行った．以降，本稿では簡単のため，この型の多数決回路のことを単に回路と呼ぶ．

3.1　1 層目ゲートの入力

1 層目ゲートの入力において変数の重複を許さない場合には，文献 [4] により回路が構成し得ないということが証明されているため，重複を許して考える．各 1 層目ゲートの入力において重複を許す場合，入力として与えられる変数には，さまざまな組合せが存在する．

例として，文献 [4] により発見された $n = 7$ の場合の回路を図 1 として示す．入力変数 $\boldsymbol{x} = (x_1, x_2, \ldots, x_7)$ である．

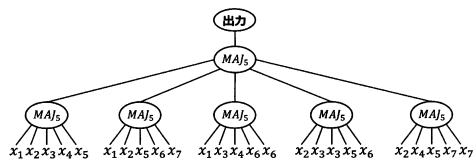


図 1: 2 層の多数決回路 $(n = 7)$

本稿を通じて，図 1 のような 2 層の多数決回路を以下のような数値列で表す．以下の数値列は，図 1 の多数決回路を表している．各 [ ] が 1 つの 1 層目ゲートを表し，その中の数字が各ゲートの入力変数の添え字を表している．

$$[1,2,3,4,5]\ [1,2,5,6,7]\ [1,3,4,6,6]$$
$$[2,3,3,5,6]\ [2,4,5,7,7]$$

3.2　2 層の多数決回路探索 $(n = 7)$

入力数 $n = 7$ について，計算機を用いて $\mathrm{MAJ}_5 \circ \mathrm{MAJ}_5$ 回路を全探索し，正しく MAJ_7 を計算しているものを列挙した．各 1 層目ゲートは 7 つの変数から 5 つを重複を許して選択するので ${}_7H_5 = 462$ 通りの

場合があり，出力ゲートはこれらから 5 個選択するので，回路の総数は ${}_{462}H_5 \sim 1.8\times10^{11}$ となる．探索の高速化を図るため，入力変数 $\boldsymbol{x} = (x_1, x_2, \ldots, x_7)$ のとり得る全ての場合で，1 層目ゲートの出力が一致しているときの 1 層目ゲートの入力を同じものと判断し，統合した．

前述の探索高速化手法における入力組合せとして，次のようなものが挙げられる．

i) $[1,1,1,1,1]$ と $[1,1,1,1,2]$ と $[1,1,1,2,3]$

ii) $[1,1,2,2,3]$ と $[1,1,2,3,3]$ と $[1,2,2,3,3]$

例えば，i) の 3 通りはいずれも x_1 の値を出力し，ii) の 3 通りはいずれも x_1, x_2, x_3 の多数決を計算する．高速化手法を適用した結果，探索する回路の総数は約 3.0×10^9 通りとなった．

$n = 7$ における多数決回路探索の結果は以下の通りである．ここで，変数の入れ替え等で等価となる組み合わせについては，本質的に同じものとみなし省いてある．

多数決回路となった組合せ (本質的に)20 通り

実行時間 約 10 時間

探索環境

CPU Intel Core i7-6700K メモリ 32GB

Windows10 64bit

4 2 層の多数決回路一般化

本研究では，前章で求めた $n = 7$ の 2 層の多数決回路の中から，3 種類の回路をもとに一般化した．まずこれらの回路を 4.1 節に示し，次に 4.2 節から 4.4 節において，それぞれの回路の特徴および一般化した回路を示す．また，本稿ではそのうちの一つ (4.3 節で示す回路) に対する正当性を証明する (5 章)．残り 2 つの回路の正当性の証明については本稿では省略する (4.2 節で示す回路の正当性の証明は [2] にある．4.4 節に示す回路の正当性はページの都合上省略する)．

4.1 一般化に成功した回路 ($n = 7$)

一般化に成功した回路は下記の 3 種類である．それらの回路をそれぞれ，回路 A_7，回路 B_7，回路 C_7 とする．

回路 A_7 ： $[3,4,5,6,7]$ $[1,1,4,6,7]$ $[2,4,4,6,7]$ $[1,2,3,6,7]$ $[1,2,3,4,5]$

回路 B_7 ： $[1,1,2,2,3]$ $[1,3,4,5,6]$ $[2,3,4,5,7]$ $[5,5,6,6,7]$ $[1,2,4,6,7]$

回路 C_7 ： $[1,1,1,1,1]$ $[2,2,3,6,7]$ $[3,3,4,6,7]$ $[4,4,5,6,7]$ $[5,5,2,6,7]$

4.2 回路 A_7

回路 A_7 の最大の特徴として，1 層目のゲートへの入力において，入力変数の重複が 2 つであることが挙げられる．回路 A_7 を表 1 として示す．表の縦軸は，入力変数 $\boldsymbol{x}$ の変数番号，横軸は，計 5 個存在する 1 層目のゲートのラベル名，各要素は，それぞれの 1 層目のゲートに指定される変数が何回入力されているかを示している．以降，回路を示す場合に表 1 と同様な形式で説明する．

表 1: 回路 A_7 の各 1 層目ゲートにおける入力の個数

	1	2	3	4	5	6	7
1	0	0	1	1	1	1	1
2	**2**	0	0	1	**0**	1	1
3	**0**	1	0	0	**2**	1	1
4	1	1	1	0	0	1	1
5	1	1	1	1	1	0	0

表 1 より，各 1 層目ゲートに欠けている (表上では 0 が記述) 入力変数，さらに太字で示されている要素には規則性がある，ということが推測される．以上の法則性から $n = 2k+1$ の場合における一般化した回路を表 2 として示す．尚，表 2 において要素が空白の箇所は全て 1 が記述されているとする．この回路は，$k \geq 3$ のとき成り立つ．

表 2: 回路 A_7 をもとに一般化した回路

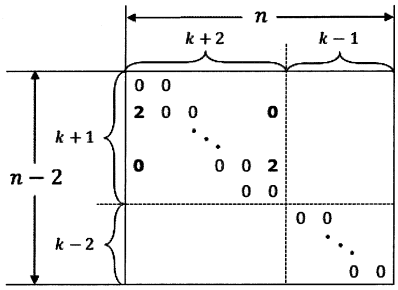
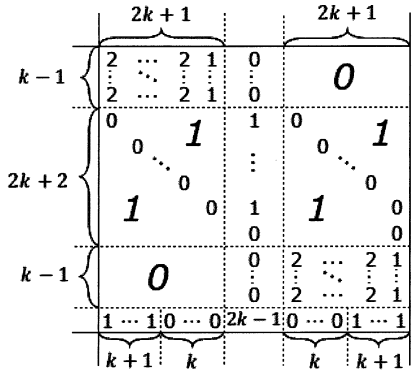


表 3: 回路 B_7 をもとに一般化した回路



4.3 回路 B_7

回路 B_7 の 1 層目ゲートには以下のような特徴がある.

- [1, 1, 2, 2, 3]
  入力変数 $\boldsymbol{x}$ の最初の 3 ビットのみの入力で構成されているゲート
- [5, 5, 6, 6, 7]
  $\boldsymbol{x}$ の最後の 3 ビットのみの入力で構成されているゲート
- [1, 3, 4, 5, 6], [2, 3, 4, 5, 7]
  入力変数の重複が存在しないゲート
- [1, 2, 4, 6, 7]
  $\boldsymbol{x}$ の最初と最後の 2 ビット, かつ中央の 1 ビットの入力で構成されているゲート

以上の法則性により, $n = 4k+3$ の場合において一般化した回路を表 3 として示す. この回路は, $k \geq 2$ のとき成り立つ. 尚, 表中の大斜体 *0,1* は, その範囲の要素が全て 0 または 1 であることを表している.

本稿では, 一般化した回路のうち回路 B_7 をもとに一般化した回路 (表 3) に着目し, より詳しい証明を与える.

$n = 4k+3$ とおく. このとき,

$$w_i \in \mathbb{N}^n \ (1 \leq i \leq 4k+1)$$

を以下のように定める.

$$w_i = \begin{cases} (\underbrace{2,2,\ldots,2}_{2k},1,0,\ldots,0) \\ (i = 1,\ldots,k-1) \\ (\underbrace{1,\ldots,1}_{i-k},0,\underbrace{1,\ldots,1}_{2k+1},0,\underbrace{1,\ldots,1}_{3k-i}) \\ (i = k,\ldots,3k) \\ (\underbrace{1,\ldots,1}_{2k+1},0,\underbrace{1,\ldots,1}_{2k},0) \\ (i = 3k+1) \\ (0,\ldots,0,\underbrace{2,2,\ldots,2}_{2k},1) \\ (i = 3k+2,\ldots,4k) \\ \underbrace{1,\ldots,1}_{k+1},\underbrace{0,\ldots,0}_{k},2k-1,0,\ldots,0,\underbrace{1,\ldots,1}_{k+1}) \\ (i = 4k+1) \end{cases} \tag{1}$$

各 1 層目ゲートをそれぞれ $m_1,\ldots,m_{4k+1}$ と表し,

$$m_i(\boldsymbol{x}) = \mathbf{1}[\sum_{1 \leq j \leq n} w_j x_j \geq 2k+1]$$

と定める．出力ゲートは，これらの単純な多数決

$$\mathbf{1}[\sum_{1\leq j\leq n-2} m_j(\boldsymbol{x}) \geq 2k+1]$$

とする．

定理 1 $n=4k+3$ $(k\geq 2)$ のとき，回路は多数決関数 MAJ_n を計算する．

定理 1 の証明に関しては第 5 章にて記述する．

4.4 回路 C_7

回路 C_7 の各 1 層目ゲートへの入力となっている入力変数 $\boldsymbol{x}=(x_1,x_2,\ldots,x_7)$ には以下の特徴がある．

- x_1：1 つの 1 層目ゲートのみへの入力となっている．
- $x_2,\ldots,x_5$：x_1 が入力として与えられていないゲートにおいて，各ゲートに 2 変数ずつ入力されており，片方の変数が重複した 2 つの入力となり，別の変数が 1 つの入力となっている (例：$[\mathbf{2},\mathbf{2},\mathbf{3},6,7]$(太字))．
- x_6,x_7：x_1 が入力として与えられていないゲートにおいて，それ以外の全てのゲートへ 1 つずつの入力となっている (例：$[2,2,3,\mathbf{6},\mathbf{7}]$(太字))．

また，回路 C_7 の特徴を図 2 に示す．これは，回路を構成する 1 層目ゲートへの入力の特徴は同じだが，正しく MAJ_7 を計算する回路ならびに計算しない回路の違いを示したものである．

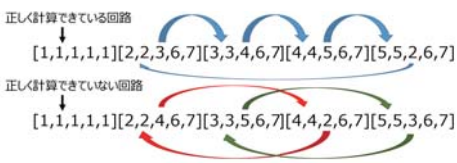
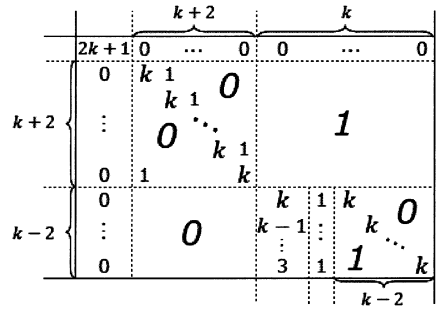


図 2: 回路 C_7 の特徴

$n=2k+3$ の場合の一般化した回路を表 4 として示す．この回路は，$k\geq 2$ のとき成り立つ．

表 4: 回路 C_7 をもとに一般化した回路



5 定理 1 に対する証明

一般化に伴い，$n=4k+3$ の場合を考える．ここで，$4k+1$ 個存在する 1 層目ゲートをそれぞれ $m_1,\ldots,m_{4k+1}$ と呼ぶ．$n=4k+3$ の場合に構成される 1 層目ゲートのうち，m_{4k+1} 以外のゲートを表 5 として示す．また，m_{4k+1} を表 6 として示す．表 5 と表 6 で 1 つの回路を表している．出力ゲートは，$m_1,m_2,\ldots,m_{4k+1}$ を入力とする多数決ゲートで，その出力は，

$$\mathbf{1}[\sum_{1\leq i\leq 4k+1} m_i(\boldsymbol{x}) \geq 2k+1]$$

となる．

以下，$m_1,\ldots,m_{k-1}$ を M_L，$m_{3k+2},\ldots,m_{4k}$ を M_R とおく．両者に含まれない，$m_k,\ldots,m_{3k+1}$ の関係性をグラフ化したものを図 3 に示す．グラフ上の頂点は，入力変数 $\boldsymbol{x}$ の添え字を表しており，辺が $m_k,m_{k+1},\ldots,m_{3k+1}$ を表している．そして，このグラフはそれぞれの 1 層目ゲートに存在しない入力変数を辺で結んでいる．また，ビット列 $\boldsymbol{x}$ に対して，$|\boldsymbol{x}|$ で $\boldsymbol{x}$ に含まれる 1 の個数を表すこととする．

ここで，$\boldsymbol{x}\in\{0,1\}^{4k+3}$ に対して，最初の $2k+1$ ビットを $\boldsymbol{x}_A$，最後の $2k+1$ ビットを $\boldsymbol{x}_B$ とおく．すなわち，$\boldsymbol{x}_A$ は，図 3 のグラフの上側，$\boldsymbol{x}_B$ は，下側にそれぞれ対応する．

表 5: $m_1, \ldots, m_{4k}$ における入力の個数

	1	2	3	…	$2k$	$2k+1$	$2k+2$	$2k+3$	$2k+4$	$2k+5$	…	$4k+3$
m_1	2		…		2	1	0	0			…	0
⋮	⋮		⋱		⋮	⋮	⋮	⋮			⋱	⋮
m_{k-1}	2		…		2	1	0	0			…	0
m_k	0	1	1		…	1	1	0	1	1	…	1
m_{k+1}	1	0	1					1	0	1		
m_{k+2}	1	1	0			⋮		1	1	0		⋮
⋮	⋮			⋱			⋮	⋮			⋱	
m_{3k-1}					0	1					0	1
m_{3k}					1	0	1				1	0
m_{3k+1}	1			…	1	1	0	1		…	1	0
m_{3k+2}	0			…		0	0	2		…	2	1
⋮	⋮			⋱		⋮	⋮	⋮		⋱	⋮	⋮
m_{4k}	0			…		0	0	2		…	2	1

表 6: m_{4k+1} における入力の個数

	1	…	$k+1$	$k+2$	…	$2k+1$	$2k+2$	$2k+3$	…	$3k+2$	$3k+3$	…	$4k+3$
m_{4k+1}	1	…	1	0	…	0	$2k-1$	0	…	0	1	…	1

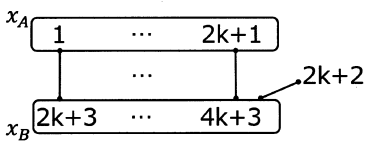


図 3: $m_k, \ldots, m_{3k+1}$ の関係性を表したグラフ

以下で，入力変数 $|\boldsymbol{x}| = 2k+2$ のときの全パターンで，

$$\sum_{1 \le i \le 4k+1} m_i(\boldsymbol{x}) \ge 2k+1$$

であることを証明する．この場合にだけ確かめれば充分であることは，以下の観察による: $|\boldsymbol{x}| = 2k+1$ の場合は，構成する回路の各ゲートが計算する $(n-2)$ 変数多数決関数の自己双対性により，$|\boldsymbol{x}| = 2k+2$ の場合から導かれる．これら両者以外の場合は，構成する回路の単調性より従う．

さて，$|\boldsymbol{x}| = 2k+2$ のとき，以下の事実が成立する．

事実 2 $|\boldsymbol{x}| = 2k+2$ のとき，図 3 のグラフの辺と接している頂点が両方とも真のときのみ，その辺は偽となる．

証明 $m_1, \ldots, m_{4k+1}$ は，入力における真の個数が $2k+1$ 以上のとき真となる．また，図 3 のグラフで辺となっている $m_k, \ldots, m_{3k+1}$ の特徴として，要素に重複がなく，$\boldsymbol{x}$ から 2 種類の要素が欠けている状態である．よって，$|\boldsymbol{x}| = 2k+2$ のとき，グラフで辺となっている $m_3, \ldots, m_{4k+1}$ を偽にするためには，欠けている 2 種類の要素が真でなければならない．以上により示された． □

事実 3 $|\boldsymbol{x}| = 2k+2$ のとき，(M_Lの全てが真) または (M_Rの全てが真) のどちらかが成り立つ．

証明　$\boldsymbol{x}_A, \boldsymbol{x}_B$ の定義より，$|\boldsymbol{x}| = 2k+2$ のとき，$|\boldsymbol{x}_A| \geq k+1$ か $|\boldsymbol{x}_B| \geq k+1$ のどちらかが成り立つことは明らかである．前者のとき，M_L の全てが真であり，後者のとき，M_R の全てが真である．以上により示された．□

補題 4 $|\boldsymbol{x}| = 2k+2$ のとき，図 3 のグラフにおいて，偽を出力する辺の数が k 以下のとき，回路の出力は真となる．

証明　事実 3 より，(M_Lの全てが真) または (M_Rの全てが真) のどちらかは成り立つので，その他の 1 層目ゲートが $k+2$ 個以上真を出力すれば，回路の出力は真となる．

図 3 のグラフは，辺の数が $2k+2$ であるため，この辺のうち $k+2$ 以上の辺が真のとき，すなわち，偽を出力する辺の数が k 以下のとき，回路の出力は真となる．以上により示された．□

本証明は，$|\boldsymbol{x}_A| \geq k+2$，$|\boldsymbol{x}_A| \leq k-1$，$|\boldsymbol{x}_A| = k+1$，$|\boldsymbol{x}_A| = k$ の 4 通りに分けて行う．

$\underline{|\boldsymbol{x}_A| \geq k+2 \text{ の場合}}$

いずれの場合も，$|\boldsymbol{x}_B| \leq k$ なので，事実 2 より，$m_k, \ldots, m_{3k+1}$ のうち，偽となる個数が k を超えることはない．よって補題 4 より，$|\boldsymbol{x}_A| \geq k+2$ の場合，回路は正しく真を出力する．

$\underline{|\boldsymbol{x}_A| \leq k-1 \text{ の場合}}$

いずれの場合も，$|\boldsymbol{x}_B| \geq k+2$ なので，事実 2 より，$m_k, \ldots, m_{3k+1}$ のうち，偽となる個数が k を超えることはない．よって補題 4 より，$|\boldsymbol{x}_A| \leq k-1$ の場合，回路は正しく真を出力する．

$\underline{|\boldsymbol{x}_A| = k+1 \text{ の場合}}$

$|\boldsymbol{x}_A| = k+1$ の場合のみ，$|\boldsymbol{x}_A| = k+1$ かつ $|\boldsymbol{x}_B| = k+1$ となる可能性がある．このとき，以下の補題が成立する．

補題 5 $|\boldsymbol{x}| = 2k+2$ のとき，M_L, M_R が共に全て真ならば，回路の出力は真となる．

証明　M_L, M_R が共に全て真のとき，回路の出力を真にするために必要な真を出力する 1 層目ゲートの個数は，これら以外に 3 個となる．

M_L, M_R が共に全て真となるのは，$|\boldsymbol{x}_A| = k+1$ かつ $|\boldsymbol{x}_B| = k+1$ の場合のみである．このとき，事実 2 より，いずれの場合も偽を出力する辺は $k+1$ 以下であるので，真を出力する辺の数が必ず $k+1$ よりも多くなる．以上により示された．□

また，$|\boldsymbol{x}_A| = k+1$ と，後に考える $|\boldsymbol{x}_A| = k$ の場合，m_{4k+1} を考慮する必要がある．m_{4k+1} には以下の補題が成立する．

補題 6 図 3 のグラフにおいて，偽を出力する辺の数が $k+1$ であると仮定する．このとき，$|\boldsymbol{x}| = 2k+2$ かつ，x_{2k+2} が真ならば，m_{4k+1} は真となる．

証明　m_{4k+1} においては，x_{2k+2} が真ならば，その時点で真の個数が $2k-1$ となる．表 6 より，m_{4k+1} への入力が 0 の入力変数の数は，$2k$ となる．それらの入力が全て真となり，かつそれら以外の入力が 1 つ真の場合のみ，x_{2k+2} が真のときに m_{4k+1} が偽となる．

しかし，これらの場合はいずれも，図 3 のグラフにおいて，偽を出力する辺の数が 2 を超えることはない．よって，x_{2k+2} が真のときに m_{4k+1} が偽となる $\boldsymbol{x}$ の真の入力の組み合わせでは，仮定と矛盾することになる．以上により示された．□

$|\boldsymbol{x}_A| = k+1$ の場合では，$x_{2k+2} = 0$，$x_{2k+2} = 1$ の 2 通りに分けて証明する．

$\underline{x_{2k+2} = 0 \text{ のとき}}$

いずれの場合も，$|\boldsymbol{x}_B| = k+1$ となるので，補題 5 より，$|\boldsymbol{x}_A| = k+1$ かつ，$x_{2k+2} = 0$ の場合，回路は正しく真を出力する．

$\underline{x_{2k+2} = 1 \text{ のとき}}$

いずれの場合も，$|\boldsymbol{x}_B| = k$ となる．事実 2 かつ事実 3 より，$m_1, \ldots, m_{4k}$ のうち，真となる個数が $2k$ となってしまう場合がある．ここで，補題 6 より，m_{4k+1} は真となるので，$m_1, \ldots, m_{4k+1}$ のうち，真となる個数は $2k+1$ となる．したがって，$|\boldsymbol{x}_A| = 2k+2$ かつ，$x_{2k+2} = 1$ の場合，回路は正しく真を出力する．

$|\boldsymbol{x}_A| = k$ の場合

$|\boldsymbol{x}_A| = k$ の場合では，$|\boldsymbol{x}_A| = k+1$ の場合と同様に 2 通りに分けて証明する．

$x_{2k+2} = 0$ のとき

いずれの場合も，$|\boldsymbol{x}_B| = k+2$ となるので，事実 2 より，$m_k, \ldots, m_{3k+1}$ のうち，偽となる個数が k を超えることはない．よって，補題 4 より，$|\boldsymbol{x}_A| = k$ かつ，$x_{2k+2} = 0$ の場合，回路は正しく出力する．

$x_{2k+2} = 1$ のとき

いずれの場合も，$|\boldsymbol{x_B}| = k+1$ となる．事実 2 かつ事実 3 より，$m_1, \ldots, m_{4k}$ のうち，真となる個数が $2k$ となってしまう場合がある．ここで，補題 6 より，m_{4k+1} は真となるので，$m_1, \ldots, m_{4k+1}$ のうち，真となる個数は $2k+1$ となる．したがって，$|\boldsymbol{x}_A| = k$ かつ，$x_{2k+2} = 1$ の場合，回路は正しく真を出力する．

以上より，一般化した回路は正しく多数決関数 MAJ_n を計算しているため，定理 1 は成立する．

6　まとめと今後の課題

本稿では，$(n, m) = (7, 5)$ について正しく MAJ_7 を計算する回路の探索を行った．その結果，多数決回路となり得る入力の組合せは，計 20 通りとなった．その後，探索した結果得られた回路をもとに，$(n, m) = (n, n-2)$ に対して，MAJ_n を計算する $\mathrm{MAJ}_m \circ \mathrm{MAJ}_m$ 回路を 3 通り与えた．そしてそれらの回路に対して，正当性を証明した．

本稿では，$(n, m) = (7, 5)$ について多数決回路の全探索を行っているが，$n \geq 9$ については探索することができていない．よって今後の課題としては，多数決回路探索におけるプログラムの改良が挙げられる．また，本稿では，$(n, m) = (n, n-2)$ について考えたが，回路を一般化していく過程で，n が大きくなる程 MAJ_n 関数を計算する $\mathrm{MAJ}_m \circ \mathrm{MAJ}_m$ 回路となるための条件が緩和されていることがわかった．そのことから，入力数が $n-k$ $(k \geq 4)$ における多数決回路の探索も今後の課題として挙げられる．

参考文献

[1] K. Amano, Bounds on the Size of Small Depth Circuits for Approximating Majority, Proc. of ICALP 2009, LNCS 5555, 39–50 (2009)

[2] K. Amano and M. Yoshida, Depth two $(n-2)$-majority circuit for n-majority, *to appear in IEICE Trans. Fund.* (2018) (available at `www.cs.gunma-u.ac.jp/~amano/paper/maj_v2.pdf`)

[3] C. Engels, M. Garg, K. Makino and A. Rao, On Expressing Majority as a Majority of Majorities, ECCC, Report No. 174 (2017)

[4] A. S. Kulikov and V. V. Podolskii, Computing Majority by Constant Depth Majority Circuits with Low Fan-in Gates, Proc. of STACS 2017, Article No.49, 49:1–49:14 (2017)

[5] R. O'Donnell and K. Wimmer, Approximation by DNF: Examples and Counter-examples, Proc. of ICALP 2007, LNCS 4596, 195–206 (2007)

[6] G. I. Posobin, Computing Majority with Low-fan-in Majority Queries, `arXiv:1711.10176` (2017)

[7] B. Rossman and S. Srinivasan, Separation of $\mathrm{AC}^0[\oplus]$ Formulas and Circuits, Proc. of ICALP 2017, Article No.50, 50:1–50:13 (2017)

[8] L. G. Valiant, Short Monotone Formulae for the Majority Function, J. Algorithms, 5(3), 363–366 (1984)